DARPATECH
2000
ISO

Information Assurance & Survivability

Brian Witten

Information Systems Office

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 074-0188*

1. AGENCY USE ONLY (Leave blank)	**2. REPORT DATE** 9/21/2000	**3. REPORT TYPE AND DATES COVERED** Briefing 9/21/2000

4. TITLE AND SUBTITLE Information Assurance & Survivability	**5. FUNDING NUMBERS**
6. AUTHOR(S) Witten, Brian	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) DARPATECH 2000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) IATAC 3190 Fairview Park Drive Falls Church, VA 22042	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; Distribution unlimited	**12b. DISTRIBUTION CODE** A

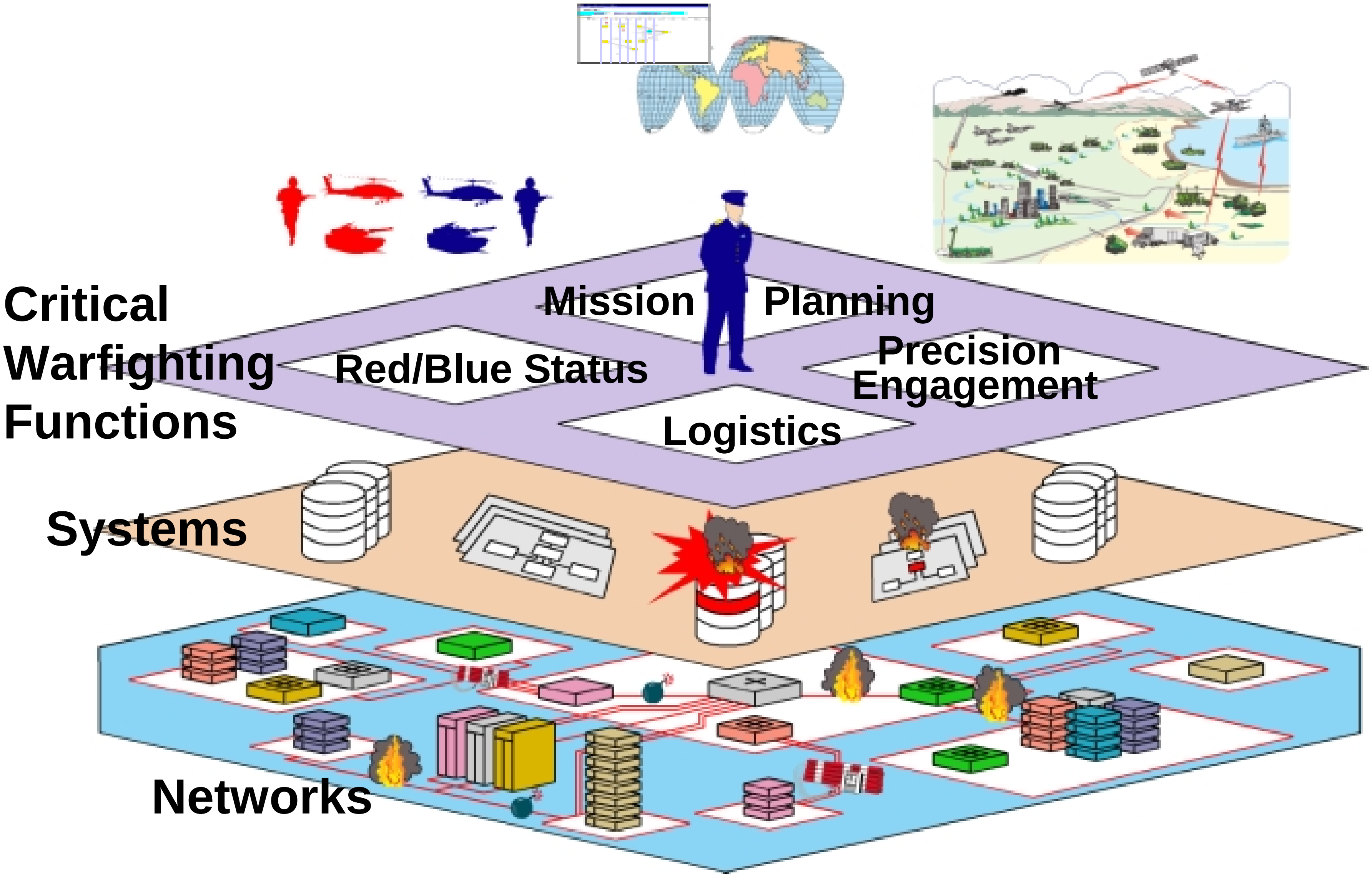
13. ABSTRACT ***(Maximum 200 Words)***

14. SUBJECT TERMS IATAC Collection, information assurance, warfighter, malicious code, mobile agents	**15. NUMBER OF PAGES** 11
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	**18. SECURITY CLASSIFICATION OF THIS PAGE** UNCLASSIFIED	**19. SECURITY CLASSIFICATION OF ABSTRACT** UNCLASSIFIED	**20. LIMITATION OF ABSTRACT** UNLIMITED

DARPATECH 2000 ISO

Can we trust the data we are fighting on?



Critical Warfighting Functions

Mission Planning

Red/Blue Status

Precision Engagement

Logistics

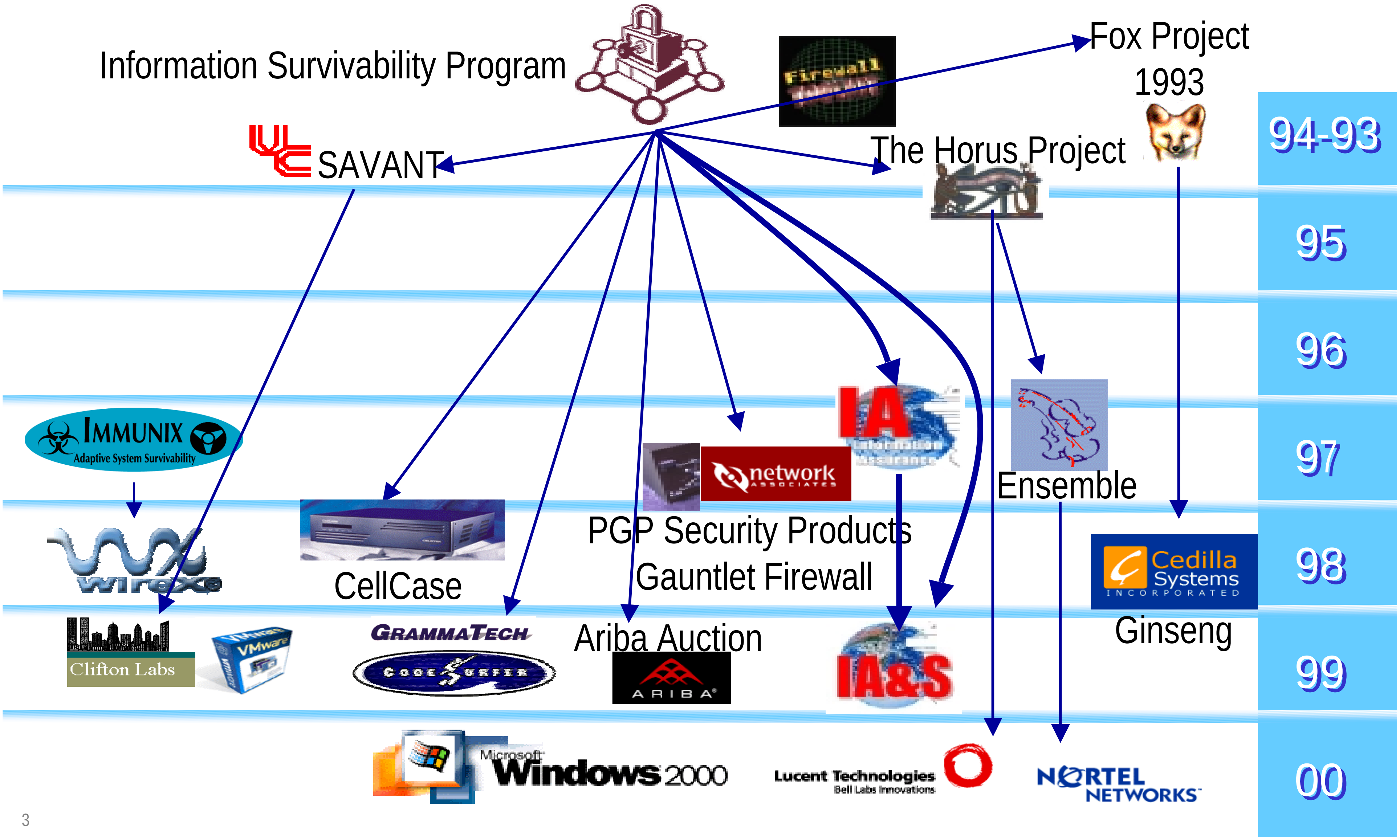
Systems

Networks

DARPATECH 2000 ISO

History of Innovations

IS Conference Proceedings - http://schafercorp-ballston.com/discex



Information Survivability Program

Fox Project
1993

SAVANT

The Horus Project

Ensemble

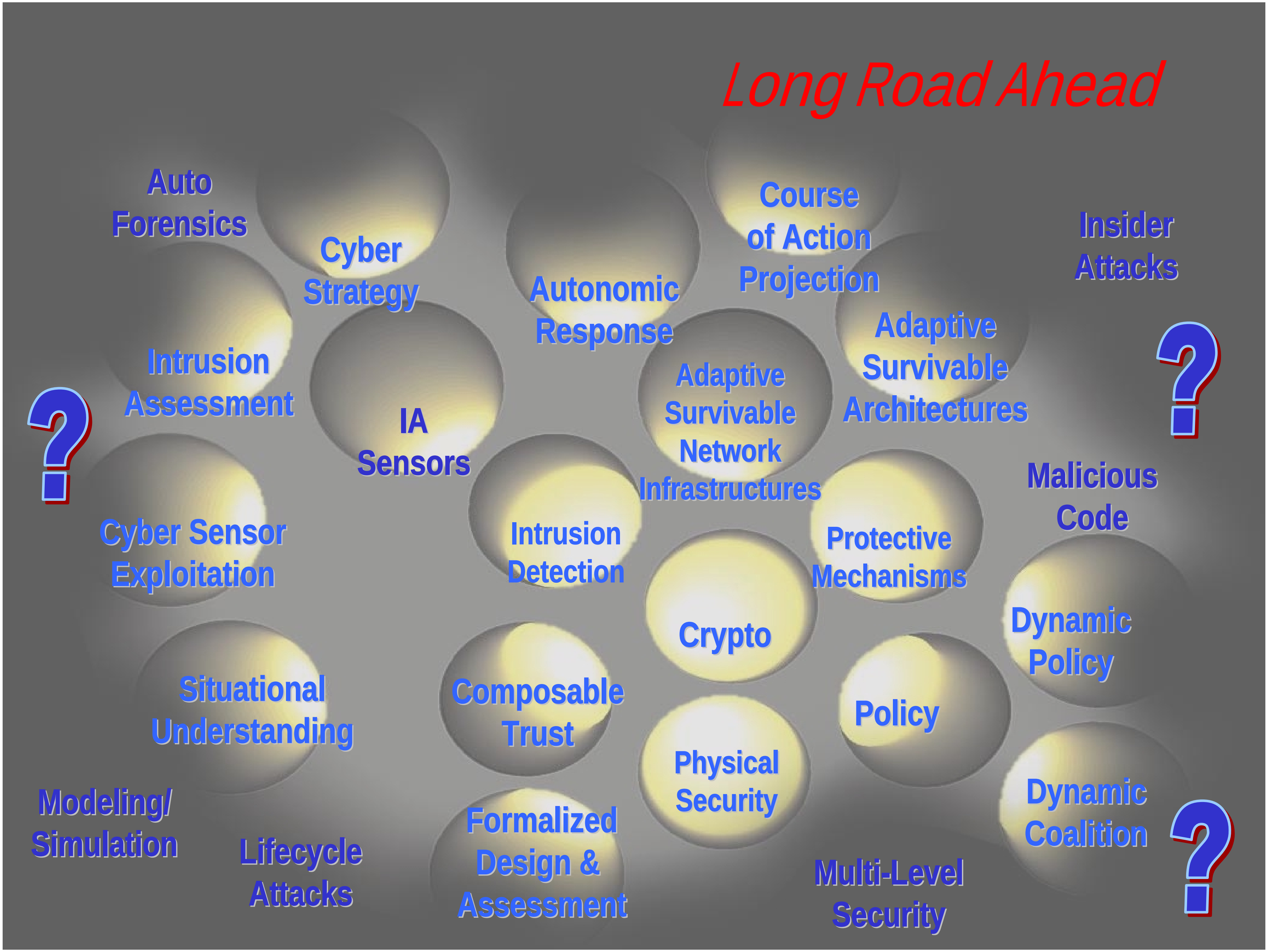
PGP Security Products
Gauntlet Firewall

CellCase

Ginseng

Ariba Auction

Long Road Ahead



Auto Forensics

Cyber Strategy

Autonomic Response

Course of Action Projection

Insider Attacks

Intrusion Assessment

IA Sensors

Adaptive Survivable Network Infrastructures

Adaptive Survivable Architectures

Cyber Sensor Exploitation

Intrusion Detection

Protective Mechanisms

Malicious Code

Crypto

Dynamic Policy

Situational Understanding

Composable Trust

Policy

Physical Security

Modeling/ Simulation

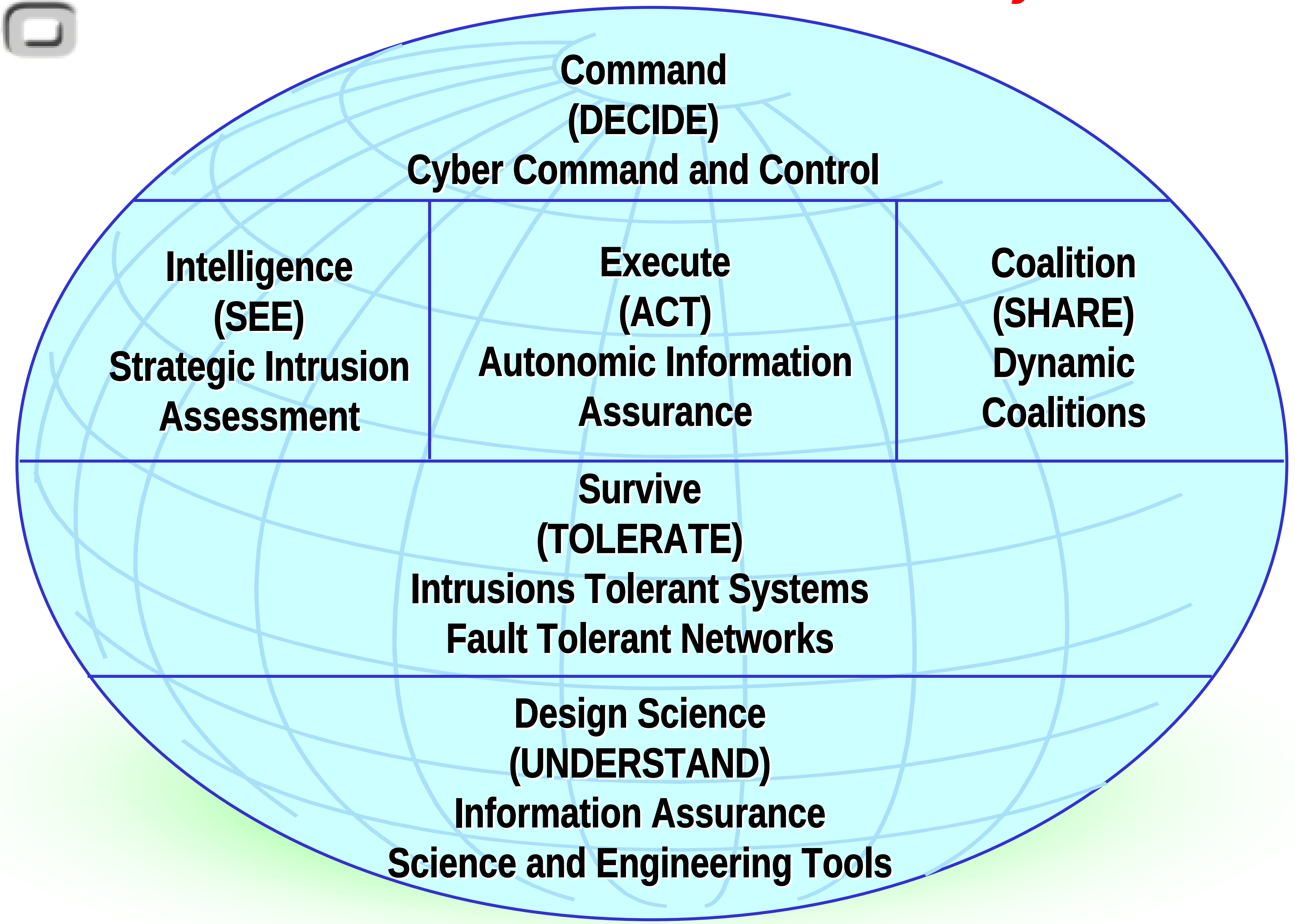
Lifecycle Attacks

Formalized Design & Assessment

Multi-Level Security

Dynamic Coalition

Objectives



Command
(DECIDE)
Cyber Command and Control

Intelligence
(SEE)
Strategic Intrusion Assessment

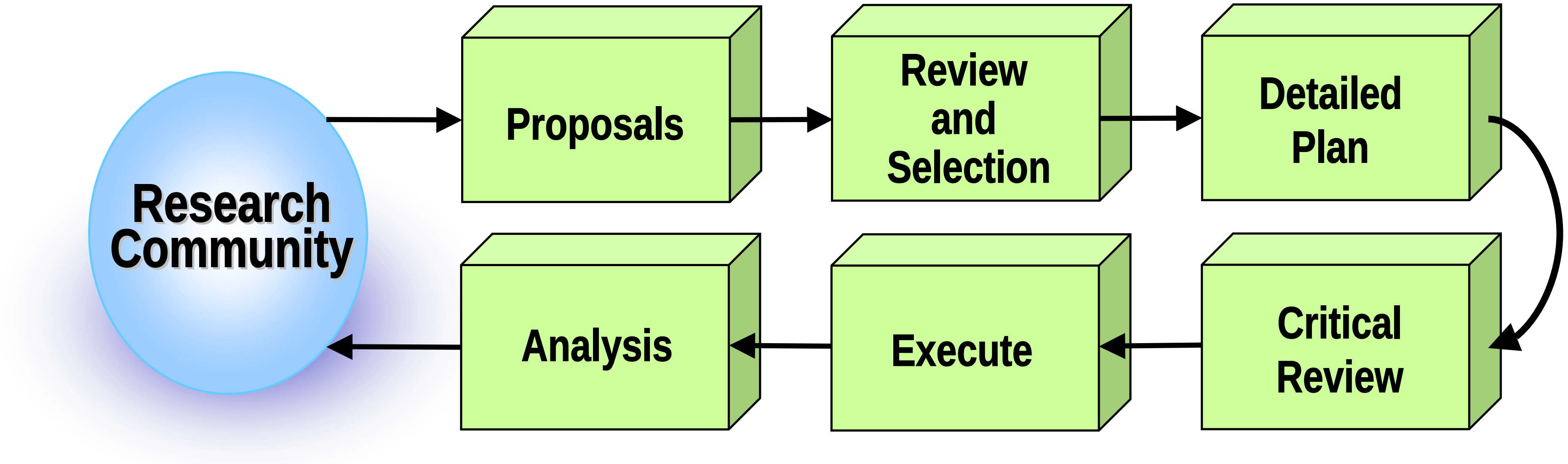
Execute
(ACT)
Autonomic Information Assurance

Coalition
(SHARE)
Dynamic Coalitions

Survive
(TOLERATE)
Intrusions Tolerant Systems
Fault Tolerant Networks

Design Science
(UNDERSTAND)
Information Assurance
Science and Engineering Tools

Approach: Scientific Experimentation



Grand Hypotheses:

- Layered Defense
- Dynamic Defense
- Assurance Methodology
- Automated Response
- Automated Decision Support

Types of Experiments:

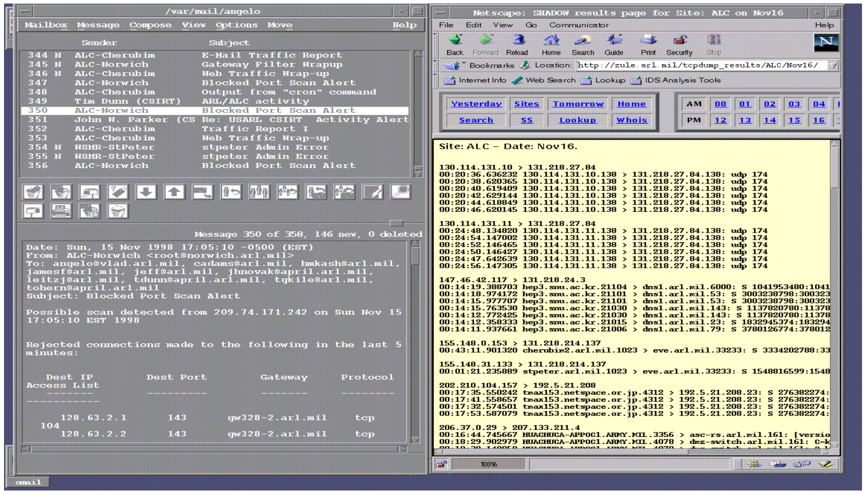
- Field Experiments
- Red Team Lab Exercise
- Laboratory Experiments
- Interdisciplinary White-Boarding
- Component Specific Testing

Contact

Autonomic Information Assurance Dynamic response	**Brian Witten** bwitten@darpa.mil
Cyber Command & Control Human directed strategy	**Catherine McCollum** cmccollum@darpa.mil
Dynamic Coalitions Coalition policy mechanisms	**Doug Maughan** dmaughan@darpa.mil
Fault Tolerant Networks Tolerant mechanisms	**Doug Maughan** dmaughan@darpa.mil
IA Science & Engineering Tools Design tools & models	**Michael Skroch** mskroch@darpa.mil
Information Assurance Composable trust	**Michael Skroch** mskroch@darpa.mil
Intrusion Tolerant Systems Tolerant systems	**Jay Lala** jlala@darpa.mil
Strategic Intrusion Assessment Attack recognition & correlation	**Catherine McCollum** cmccollum@darpa.mil
Cyber Sensor Grid	Catherine McCollum
Malicious Code Mitigation	Michael Skroch
Reliable Mobile Agents	Brian Witten
Secure Operating Systems	Doug Maughan
Security of High Speed Networks	Doug Maughan

DARPATECH 2000 ISO

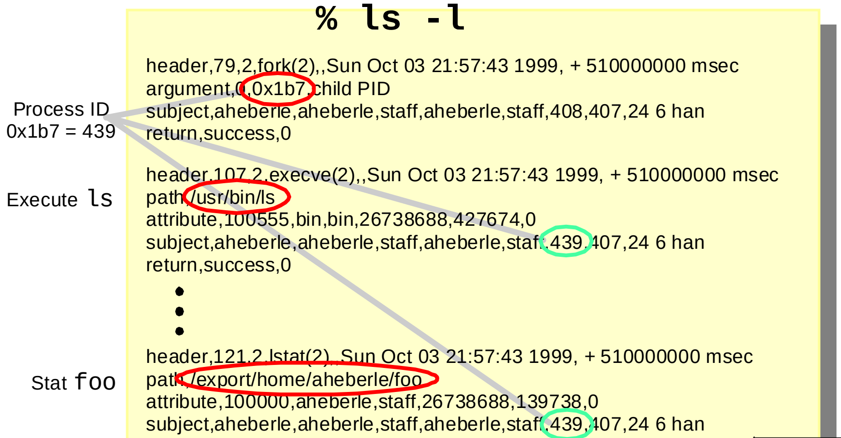
New Focus: Cyber Sensor Grid



```
/var/mail/angelo
Mailbox  Message  Compose  View  Options  Move                         Help

           Sender                    Subject
 344 N  ALC-Cherubim           E-Mail Traffic Report
 345 N  ALC-Norwich            Gateway Filter Wrapup
 346 N  ALC-Cherubim           Web Traffic Wrap-up
 347    ALC-Norwich            Blocked Port Scan Alert
 348    ALC-Cherubim           Output from "cron" command
 349    Tim Dunn (CSIRT)       ARL/ALC activity
 350    ALC-Norwich            Blocked Port Scan Alert
 351    John W. Parker (CS Re: USARL CSIRT  Activity Alert
 352    ALC-Cherubim           Traffic Report I
 353    ALC-Cherubim           Web Traffic Wrap-up
 354 N  WSMR-StPeter           stpeter Admin Error
 355 N  WSMR-StPeter           stpeter Admin Error
 356    ALC-Norwich            Blocked Port Scan Alert

                                   Message 350 of 358, 146 new, 0 deleted
Date: Sun, 15 Nov 1998 17:05:10 -0500 (EST)
From: ALC-Norwich <root@norwich.arl.mil>
To: angelo@vlad.arl.mil, cadams@arl.mil, hmkash@arl.mil,
jamesf@arl.mil, jeff@arl.mil, jhnovak@april.arl.mil,
leitzj@arl.mil, tdunn@april.arl.mil, tgkile@arl.mil,
tohern@april.arl.mil
Subject: Blocked Port Scan Alert

Possible scan detected from 209.74.171.242 on Sun Nov 15
17:05:10 EST 1998


Rejected connections made to the following in the last 5
minutes:


   Dest IP          Dest Port         Gateway      Protocol
Access List
   -------          ---------         -------      --------
----------

     128.63.2.1        143       gw328-2.arl.mil     tcp
  104
     128.63.2.2        143       gw328-2.arl.mil     tcp
```

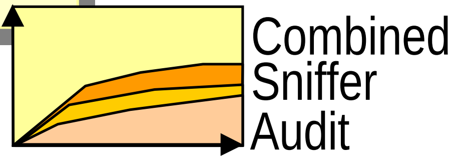
```
Netscape: SHADOW results page for Site: ALC on Nov16
File  Edit  View  Go  Communicator                                  Help
Back  Forward  Reload  Home  Search  Guide  Print  Security  Stop
Bookmarks  Location: http://zule.arl.mil/tcpdump_results/ALC/Nov16/
Internet Info  Web Search  Lookup  IDS Analysis Tools

Yesterday  Sites  Tomorrow  Home       AM  00  01  02  03  04
Search     SS     Lookup    Whois      PM  12  13  14  15  16

Site: ALC - Date: Nov16.

130.114.131.10 > 131.218.27.84
00:20:36.636232 130.114.131.10.138 > 131.218.27.84.138: udp 174
00:20:38.620365 130.114.131.10.138 > 131.218.27.84.138: udp 174
00:20:40.619409 130.114.131.10.138 > 131.218.27.84.138: udp 174
00:20:42.629144 130.114.131.10.138 > 131.218.27.84.138: udp 174
00:20:44.618849 130.114.131.10.138 > 131.218.27.84.138: udp 174
00:20:46.620145 130.114.131.10.138 > 131.218.27.84.138: udp 174

130.114.131.11 > 131.218.27.84
00:24:48.134820 130.114.131.11.138 > 131.218.27.84.138: udp 174
00:24:54.147002 130.114.131.11.138 > 131.218.27.84.138: udp 174
00:24:52.146465 130.114.131.11.138 > 131.218.27.84.138: udp 174
00:24:50.146427 130.114.131.11.138 > 131.218.27.84.138: udp 174
00:24:47.642639 130.114.131.11.138 > 131.218.27.84.138: udp 174
00:24:56.147305 130.114.131.11.138 > 131.218.27.84.138: udp 174

147.46.42.117 > 131.218.24.3
00:14:19.388703 hep3.snu.ac.kr.21104 > dns1.arl.mil.6000: S 1041953480:1041
00:14:18.974172 hep3.snu.ac.kr.21101 > dns1.arl.mil.53: S 3003238798:300323
00:14:15.977707 hep3.snu.ac.kr.21101 > dns1.arl.mil.53: S 3003238798:300323
00:14:15.763530 hep3.snu.ac.kr.21030 > dns1.arl.mil.143: S 1137820780:11378
00:14:12.772425 hep3.snu.ac.kr.21030 > dns1.arl.mil.143: S 1137820780:11378
00:14:12.358333 hep3.snu.ac.kr.21015 > dns1.arl.mil.23: S 1832945374:183294
00:14:11.937661 hep3.snu.ac.kr.21006 > dns1.arl.mil.79: S 3780126774:378012

155.148.0.153 > 131.218.214.137
00:43:11.901320 cherubim2.arl.mil.1023 > eve.arl.mil.33233: S 3334202788:33

155.148.31.133 > 131.218.214.137
00:01:21.235889 stpeter.arl.mil.1023 > eve.arl.mil.33233: S 1548816599:1548

202.210.104.157 > 192.5.21.208
00:17:35.550242 tmax153.netspace.or.jp.4312 > 192.5.21.208.23: S 276382274:
00:17:41.558657 tmax153.netspace.or.jp.4312 > 192.5.21.208.23: S 276382274:
00:17:32.574501 tmax153.netspace.or.jp.4312 > 192.5.21.208.23: S 276382274:
00:17:53.587079 tmax153.netspace.or.jp.4312 > 192.5.21.208.23: S 276382274:

206.37.0.29 > 207.133.211.4
00:16:44.745667 HUACHUCA-APPOC1.ARMY.MIL.3356 > asc-rs.arl.mil.161: [versio
00:18:29.902979 HUACHUCA-APPOC1.ARMY.MIL.4078 > dmz-switch.arl.mil.161: C=k
```

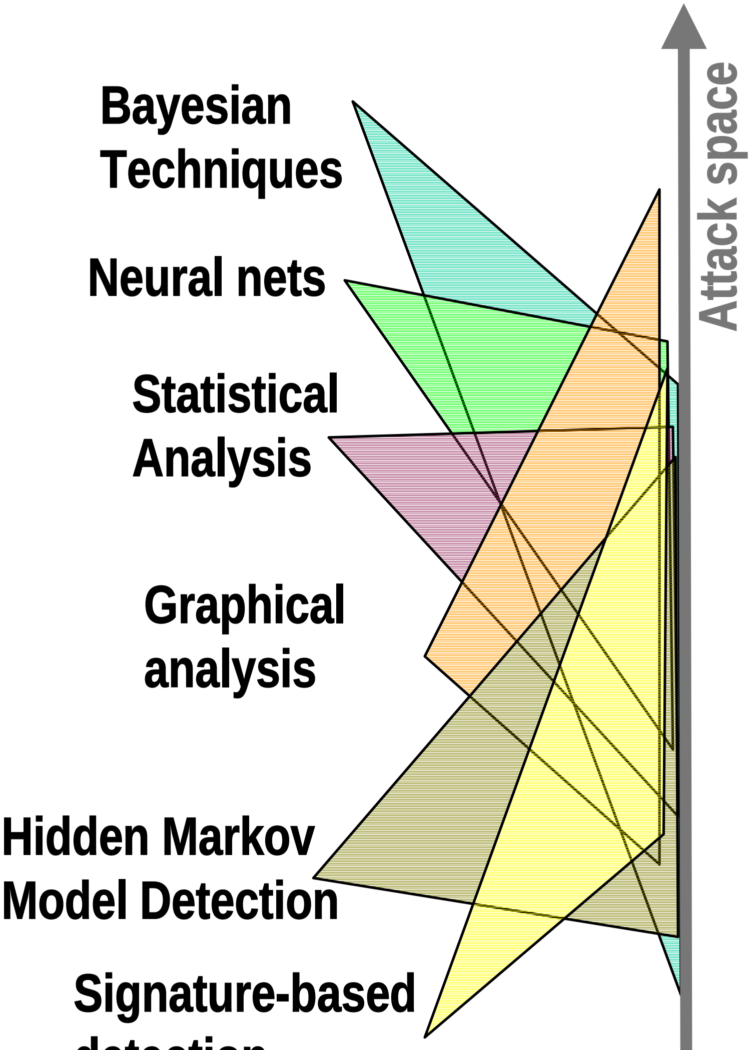
Sniffer data



```
% ls -l

header,79,2,fork(2),,Sun Oct 03 21:57:43 1999, + 510000000 msec
argument,0,0x1b7,child PID
subject,aheberle,aheberle,staff,aheberle,staff,408,407,24 6 han
return,success,0

header,107,2,execve(2),,Sun Oct 03 21:57:43 1999, + 510000000 msec
path,/usr/bin/ls
attribute,100555,bin,bin,26738688,427674,0
subject,aheberle,aheberle,staff,aheberle,staff,439,407,24 6 han
return,success,0
•
•
•
header,121,2,lstat(2),,Sun Oct 03 21:57:43 1999, + 510000000 msec
path,/export/home/aheberle/foo
attribute,100000,aheberle,staff,26738688,139738,0
subject,aheberle,aheberle,staff,aheberle,staff,439,407,24 6 han
return,success,0
```

Audit data





Bayesian Techniques

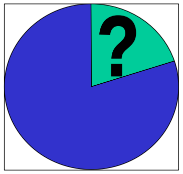
Neural nets

Statistical Analysis

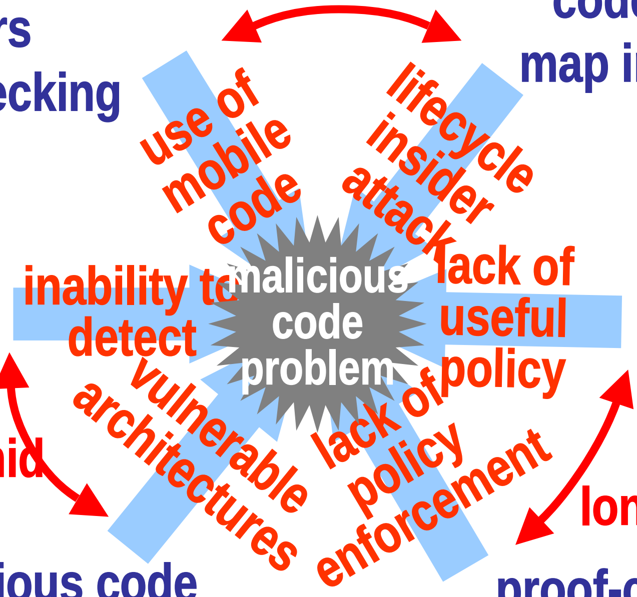
Graphical analysis

Hidden Markov Model Detection

Signature-based detection



New Focus: Malicious Code Mitigation



problem-defining
primarily
program-external

sandboxing
wrappers
integrity checking

~~cleared developers~~
code signing standard
map insider effects to MC

static code analysis
code authentication
anomaly detection
epidemiological-based

policy management tools
checking tools
policy composition

short-mid
term

theories for malicious code
tolerant architectures
bilateral trustworthy path
static & adaptive fault tolerance

long-term

proof-carrying code
theory of response

Complicating factors:
- More COTS
- Increasing use and reliance on systems
- Increasing connectivity

Strategy:
- Detect & Expunge “On the Fly”
- New Architectural Concepts
- Address Policy Language Lag

DARPATECH 2000 ISO

New Focus: Reliable Mobile Agents

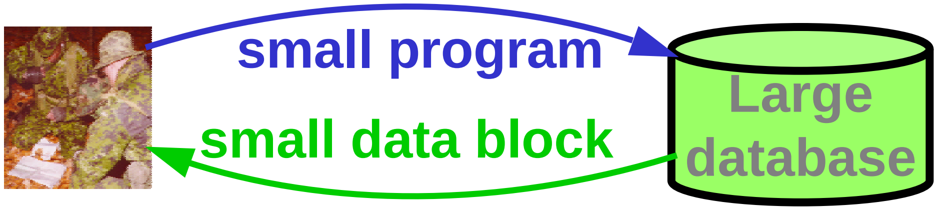
Mobile Agents are:

Programs that can migrate from machine to machine under their own control.

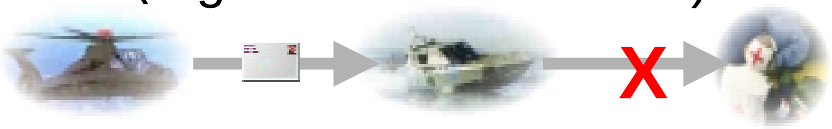
Code mobility…

Functionally enhances:

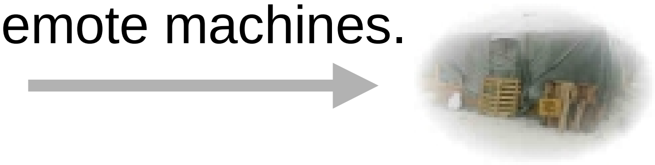
1. **Efficiency**



2. **Disconnected operations**
   (e.g.. wireless networks)

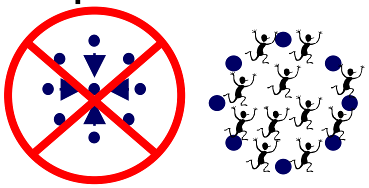


3. **Flexibility**
   Install new functionality on remote machines.



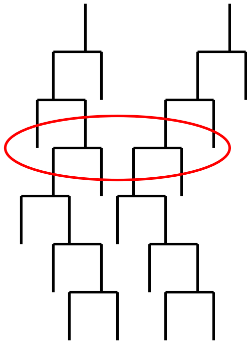
Presents Survivability Opportunities:

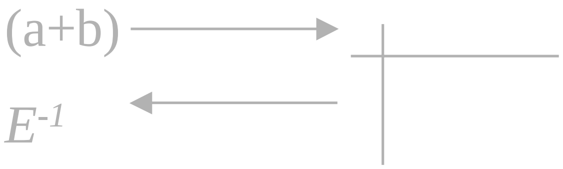
1. **Availability**
   No central failure point.



2. **Integrity**
   Fluidly reinforce execution traces.

3. **Confidentiality**
   Code fragmentation.
   Mobile cryptography.





Conclusions:

- National Level Problem
- DARPA "high-risk"/ "high-reward" focus

New Focus Areas:

- Cyber Sensor Grid
- Malicious Code Mitigation
- Reliable Mobile Agents

Proven Success:

- ARPANET
- Firewall Toolkit

Waiting Gold:

- Secure Domain Name Service
- Internet Protocol Security (IPSEC)
- Secure Border Gateway Protocol
- Next Generation Intrusion Detection

More to Come:

- Denying Denial-of-Service
- Self-Healing Systems
- Proof Carrying Code
- Trace Back
- Dynamic Defense
- Metrics & Science Based Design

IA&S Information – www.darpa.mil